Notice of Allowability	Application No.	Applicant(s)	
	09/306,227	CALLUM, ROY	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the response filed on November 8, 2004*.

2. ☒ The allowed claim(s) is/are *1-15*.

3. ☒ The drawings filed on *06 May 1999* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *February 16, 2005*.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

2/16/05

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert Anderson on February 16, 2005.

The application has been amended as follows:

Additions are underlines and omissions are bracketed

1. (Currently Amended) A circuit comprising:

a [an] DES operation unit adapted to perform a circuit operation in a plurality of rounds per clock cycle, the DES operation unit to operate properly under a predetermined range of operating conditions and not to operate if the operating conditions are altered beyond the predetermined range, the DES operation unit adapted to select between receiving an input signal and a test signal and to perform a test round per clock cycle of the circuit operation when the test signal is selected;

the circuit adapted to compare a reference value with a result of the test round per clock cycle, the reference value identifying a correct value for the result of the test round per clock cycle when the DES operation unit is operating under the predetermined range of operating conditions; and

the DES operation unit further adapted to receive a disable signal to disable the operation unit from performing the circuit operation when the operating conditions of the operating unit have been altered beyond the predetermined range, the disable signal produced when the result of the test round per clock cycle does not match the reference value;

wherein the operating conditions include at least one of an operating temperature, an operating voltage or an operating clock frequency.

4. (Currently Amended) A method comprising:

selecting a test signal to apply to a test round per clock cycle of a circuit operation performing DES, the circuit operation comprising a plurality of rounds per clock cycle;

comparing a result of the test round per clock cycle with a stored reference value, the stored reference value identifying a correct value for the result of the test round per clock cycle when the circuit is operating under a predetermined range of operating conditions; and

producing a disable signal to disable the operation unit from performing the circuit operation when the result of the test round per clock cycle does not match the reference value and when operating conditions of the circuit have been altered beyond the predetermined range of operating conditions;

wherein the operating conditions include at least one of an operating temperature, an operating voltage or an operating clock frequency.

8. (Currently Amended) A circuit comprising:

a sampling unit to produce a measure of a first frequency of a clock signal applied to the circuit that performs DES operations, wherein the DES operations produce test rounds per clock cycle;

a memory to store the measure of the first frequency; and

an analytical unit to compare the measure of the first frequency with a measure of a second frequency of the clock signal applied to the circuit producing the test round per clock cycle, the analytical unit adapted to produce a disable signal to disable the circuit when a difference, between the measure of first frequency and the measure of the second frequency exceeds a threshold value when operating conditions of the circuit have been altered beyond a predetermined range; and

an oscillator adapted to produce a frequency greater than the first and second frequencies of the clock signal;

wherein the operating conditions include at least one of an operating temperature, an operating voltage or an operating clock frequency.

13. (Currently Amended) A method comprising:

sampling a clock signal applied to a circuit to produce a first frequency sample, wherein the circuit performs DES operations, the DES operations are produced in test rounds per clock cycle;

storing the first frequency sample;

again sampling the clock signal to produce a second frequency sample;

comparing the first frequency sample with the second frequency sample of the circuit that produced the test round per clock cycle;

producing a disable signal to disable the circuit when the difference between the first frequency sample and the second frequency sample exceeds a threshold value when operating conditions of the circuit have been altered beyond a predetermined range; and

producing an oscillation comprising a frequency greater than the frequency of the clock signal;

wherein the operating conditions include at least one of an operating temperature, an operating voltage or an operating clock frequency.

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance:

As per claim 1, it was not found to be taught in the prior art of a DES operation unit adapted to perform a circuit operation in a plurality of rounds per clock cycle which operates properly under a predetermined range of operating conditions. A reference value is compared with a result of the test round per clock cycle, the reference value identifying a correct value for the result of the test round per clock cycle when the DES operation unit is operating under the predetermined range of operating conditions. The DES operation is disabled when the operating conditions have been altered beyond the

predetermined range wherein result of the test round per clock cycle does not match the reference value.

As per claim 4, it was not found to be taught in the prior art of applying a test signal to a test round per clock cycle of a circuit operation performing DES, the circuit operation comprising a plurality of rounds per clock cycle. The result of the test round per clock cycle is compared with a stored reference value, the stored reference value identifying a correct value for the result of the test round per clock cycle when the circuit is operating under a predetermined range of operating conditions. A disable signal is produced to disable the operation unit from performing the circuit operation when the result of the test round per clock cycle does not match the reference value.

As per claim 8, it was not found to be taught in the prior art of a sampling unit producing a measure of a first frequency of a clock signal applied to the circuit that performs DES operations, wherein the DES operations produce test rounds per clock cycle. The measure of the first frequency is compared with a measure of a second frequency of the clock signal applied to the circuit producing the test round per clock cycle. A disable signal is produced to disable the circuit when a difference, between the measure of first frequency and the measure of the second frequency exceeds a threshold value.

As per claim 13, it was not found to be taught in the prior art of sampling a clock signal applied to a circuit to produce a first frequency sample, wherein the circuit performs DES operations, the DES operations are produced in test rounds per clock cycle. The first frequency sample is compared with the second frequency sample of the

circuit that produced the test round per clock cycle. A disable signal is produced to disable the circuit when the difference between the first frequency sample and the second frequency sample exceeds a threshold value.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Menezes et al, "Handbook of Applied Cryptography" is a general teaching of the Data Encryption Standard.

Schneier, "Applied Cryptography" is a general teaching of the Data Encryption Standard.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

CR
February 16, 2005

2/16/05